CLAIMS

What is claimed is:

1. A method for preventing an outbreak of malicious code, comprising:

a) identifying malicious code at a local location on a network;

b) encrypting information relating to the malicious code at the local location;

c) sending the encrypted information relating to the malicious code to a plurality of remote locations utilizing the network; and

d) blocking instances of the malicious code at the remote locations for a predetermined amount of time based on the information;

e) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the malicious code.

2. The method as recited in claim 1, wherein the malicious code is at least one of a virus, worm, and Trojan.

3. The method as recited in claim 1, wherein the information relating to the malicious code includes an identification of the source of the malicious code, wherein communications originating at the identified source are denied access to the remote locations for the predetermined amount of time.

4. The method as recited in claim 1, further comprising registering at least one of a name and checksum of a file containing the malicious code as a known threat.

5. The method as recited in claim 1, further comprising executing countermeasures for limiting the effect of the malicious code at the local location.

6. The method as recited in claim 1, wherein the instances of the malicious code are identified based on at least one of a file name and a checksum of the malicious code.

7. The method as recited in claim 1, wherein additional information about the malicious code is retrieved if an aspect of the malicious code is not recognized.

8. A computer program product for managing an outbreak of malicious code, comprising:

a) computer code for identifying malicious code at a local location on a network;

b) computer code for encrypting information relating to the malicious code at the local location;

c) computer code for sending the encrypted information relating to the malicious code to a plurality of remote locations utilizing the network; and

d) computer code for blocking instances of the malicious code at the remote locations for a predetermined amount of time based on the information;

e) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the malicious code.

9. A system for preventing an outbreak of malicious code, comprising:

a) logic for identifying malicious code at a local location on a network;

b) logic for encrypting information relating to the malicious code at the local location;

c) logic for sending the encrypted information relating to the malicious code to a plurality of remote locations utilizing the network; and

d) logic for blocking instances of the malicious code at the remote locations for a predetermined amount of time based on the information;

e) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the malicious code.

10. A method for preventing an outbreak of malicious code, comprising:

a) identifying malicious code at a local location on a network;

b) gathering information relating to the malicious code at the local location;

c) sending the information relating to the malicious code to a remote location utilizing the network; and

d) blocking instances of the malicious code at the remote location;

e) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and source of the malicious code.

11. The method as recited in claim 10, wherein the malicious code is at least one of a virus, worm, and Trojan.

12. The method as recited in claim 10, wherein the instances of the malicious code are blocked at the remote location for a predetermined amount of time based on the information.

13. The method as recited in claim 10, wherein the information relating to the malicious code includes an identification of the source of the malicious code, wherein communications originating at the identified source are denied access to the remote locations.

14. The method as recited in claim 10, further comprising registering a name of a file of the malicious code as a known threat.

15. The method as recited in claim 10, wherein the malicious code is recognized based at least in part on recognizing that a source of the malicious code is registered as a known threat.

16. The method as recited in claim 10, further comprising executing countermeasures for limiting the effect of the malicious code at the local location.

17. A computer program product for preventing an outbreak of malicious code, comprising:

a) computer code for identifying malicious code at a local location on a network;

b) computer code for gathering information relating to the malicious code at the local location;

c) computer code for sending the information relating to the malicious code to a remote location utilizing the network; and

d) computer code for blocking instances of the malicious code at the remote location;

e) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and source of the malicious code.

18. A system for preventing an outbreak of malicious code, comprising:

a) logic for identifying malicious code at a local location on a network;

b) logic for gathering information relating to the malicious code at the local location;

c) logic for sending the information relating to the malicious code to a remote location utilizing the network; and

d) logic for blocking instances of the malicious code the remote location;

e) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and source of the malicious code.

19. A method for denying access to a hacker, comprising:

a) identifying an attack by a hacker at a local location on a network;

b) encrypting information relating to the attack at the local location;

c) sending the encrypted information relating to the attack to a plurality of remote locations utilizing the network; and

d) restricting access to the remote locations for a predetermined amount of time based on the information;

e) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the attack.

20. The method as recited in claim 19, wherein the attack attempts to create a denial of service.

21. The method as recited in claim 19, wherein the information relating to the attack includes an identification of the source of the attack, wherein communications originating at the identified source are denied access to the remote locations for the predetermined amount of time.

22. The method as recited in claim 21, further comprising registering the source of the attack as a known threat.

23. The method as recited in claim 19, wherein the attack is recognized based at least in part on recognizing that the source of the attack is registered as a known threat.

24. The method as recited in claim 19, further comprising executing countermeasures for limiting the effect of the attack at the local location.

25. The method as recited in claim 19, wherein additional information about the attack is retrieved if an aspect of the attack is not recognized.

26. A computer program product for denying access to a hacker, comprising:

a) computer code for identifying an attack by a hacker at a local location on a network;

b) computer code for encrypting information relating to the attack at the local location;

c) computer code for sending the encrypted information relating to the attack to a plurality of remote locations utilizing the network; and

d) computer code for restricting access to the remote locations for a predetermined amount of time based on the information;

e) for wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the attack.

27. A system for denying access to a hacker, comprising:

a) logic for identifying an attack by a hacker at a local location on a network;

b) logic for encrypting information relating to the attack at the local location;

c) logic for sending the encrypted information relating to the attack to a plurality of remote locations utilizing the network; and

d) logic for restricting access to the remote locations for a predetermined amount of time based on the information;

e) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the attack.

28. A method for denying access to a hacker, comprising:

a) identifying an attack by a hacker at a local location on a network;

b) gathering information relating to the attack at the local location;

c) sending the information relating to the attack to a remote location utilizing the network; and

d) restricting access to the remote location;

e) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and source of the attack.

29. The method as recited in claim 28, wherein the attack attempts to create a denial of service.

30. The method as recited in claim 28, wherein the access to the remote location is restricted for a predetermined amount of time based on the information.

31. The method as recited in claim 28, wherein the information relating to the attack includes an identification of the source of the attack, wherein communications originating at the identified source are denied access to the remote locations.

32 The method as recited in claim 31, further comprising registering the source of the attack as a known threat.

33. The method as recited in claim 28, wherein the attack is recognized based at least in part on recognizing that a source of the attack is registered as a known threat.

34. The method as recited in claim 28, further comprising executing countermeasures for limiting the effect of the attack at the local location.

35. A computer program product for denying access to a hacker, comprising:

a) computer code for identifying an attack by a hacker at a local location on a network;

b) computer code for gathering information relating to the attack at the local location;

c) computer code for sending the information relating to the attack to a remote location utilizing the network; and

d) computer code for restricting access to the remote location;

e) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and source of the attack.

36. A system for denying access to a hacker, comprising:

a) logic for identifying an attack by a hacker at a local location on a network;

b) logic for gathering information relating to the attack at the local location;

c) logic for sending the information relating to the attack to a remote location utilizing the network; and

d) logic for restricting access to the remote location;

e) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and source of the attack.

37. A method for preventing an outbreak of malicious code, comprising:

a) identifying malicious code at a local location on a network;

b) wherein the malicious code is at least one of a virus, worm and, Trojan;

c) wherein the malicious code is recognized based at least in part on recognizing that at least one of a checksum and a file name of the malicious code is registered as a known threat;

d) encrypting information relating to the malicious code at the local location, wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the malicious code;

e) sending the encrypted information relating to the malicious code to a plurality of remote locations utilizing the network;

f) restricting access to the remote locations by communications originating at the source of the malicious code for a predetermined amount of time based on the information;

g) executing countermeasures for limiting the effect of the malicious code at the local location; and

h) retrieving additional information about the malicious code if an aspect of the attack is not recognized.